

Docket No. SHAI-11

IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) In a system for sending messages over a network between first and second computing units, method comprising the following steps:

(a). computing r components of encrypting key $e_{\text{sub.1}}, e_{\text{sub.2}}, \dots, e_{\text{sub.r}}$ and r components of decrypting key $d_{\text{sub.1}}, d_{\text{sub.2}}, \dots, d_{\text{sub.r}}$ according to the following relations:

$$(e_{\text{sub.1}}).(d_{\text{sub.1}})+(e_{\text{sub.2}}).(d_{\text{sub.2}})+\dots+(e_{\text{sub.r}}).(d_{\text{sub.r}})=(k_{\text{sub.1}}).(p-1).(q-1)+1 \text{ and}$$

$$(d_{\text{sub.1}})+(d_{\text{sub.2}})+\dots+(d_{\text{sub.r}})=(k_{\text{sub.2}}).(p-1).(q-1), \text{ where:}$$

p and q are two prime numbers;

$k_{\text{sub.1}}$ and $k_{\text{sub.2}}$ are suitable integers; and

encrypting a message M into r cipher versions $M_{\text{sub.1}}, M_{\text{sub.2}}, \dots, M_{\text{sub.r}}$ using the r blinded components of the encrypting key $e_{\text{sub.1}}+t, e_{\text{sub.2}}+t, \dots, e_{\text{sub.r}}+t$ as follows:

$$M_{\text{sub.1}}=(M_{\text{sup.}}(e_{\text{sub.1}}+t)) \bmod n$$

$$M_{\text{sub.2}}=(M_{\text{sup.}}(e_{\text{sub.2}}+t)) \bmod n$$

...

$$M_{\text{sub.r}}=(M_{\text{sup.}}(e_{\text{sub.r}}+t)) \bmod n, \text{ where:}$$

$$n=p.q;$$

t is a random number generated on an encrypting unit and discarded after encryption is complete;

Amendment – Serial No. 09/847,503.....Page 2

Docket No. SHAI-11

mod represents the remainder left when left hand operand is divided by right hand operand;

~~— or~~

~~— computing the key components $e_{sub.1}, e_{sub.2}, \dots, e_{sub.r}$ and $d_{sub.1}, d_{sub.2}, \dots, d_{sub.r}$ according to the following relation and conditions:~~

~~— $(e_{sub.1}) \cdot (d_{sub.1}) + (e_{sub.2}) \cdot (d_{sub.2}) + \dots$~~

~~$+ (e_{sub.r}) \cdot (d_{sub.r}) = (k_{sub.1}) \cdot (p-1) \cdot (q-1) + 1$ and~~

~~— each of the values $(e_{sub.1}), (e_{sub.2}), \dots, (e_{sub.r})$ has a common factor with $(p-1) \cdot (q-1)$, but there is no common factor for all $(e_{sub.1}), (e_{sub.2}), \dots, (e_{sub.r}), (p-1) \cdot (q-1)$, where:~~

~~— p and q are prime numbers;~~

~~— $k_{sub.1}$ is a suitable integer; and~~

~~— encrypting a message M into r cipher versions $M_{sub.1}, M_{sub.2}, \dots, M_{sub.r}$ using the r components of the encrypting key, $e_{sub.1}, e_{sub.2}, \dots, e_{sub.r}$ as follows:~~

~~— $M_{sub.1} = M_{sup.}(e_{sub.1}) \bmod n$~~

~~— $M_{sub.2} = M_{sup.}(e_{sub.2}) \bmod n$~~

~~— \dots~~

~~— $M_{sub.r} = M_{sup.}(e_{sub.r}) \bmod n$, where:~~

~~— $n = p \cdot q$;~~

~~— p and q are two prime numbers;~~

Amendment – Serial No. 09/847,503.....Page 3

Docket No. SHAI-11

(b). delivering all the cipher versions of the message individually to ~~the~~ a destination unit in source routing mode, or hop-by-hop routing mode with a small time gap between every two consecutive cipher versions;

(c). collecting all the cipher versions at the destination unit;

(d). computing r number of values $N_{sub.1}$, $N_{sub.2}$, ..., $N_{sub.r}$ using r components $d_{sub.1}$, $d_{sub.2}$, ..., $d_{sub.r}$ of decrypting key, where:

$$N_{sub.1} = ((M_{sub.1})_{sup.}(d_{sub.1})) \bmod n$$

$$N_{sub.2} = ((M_{sub.2})_{sup.}(d_{sub.2})) \bmod n$$

...

$$N_{sub.r} = ((M_{sub.r})_{sup.}(d_{sub.r})) \bmod n, \text{ where:}$$

n is the same composite number as used for encryption;

(e). reproducing the original message M as follows:

$$M = (N_{sub.1}).(N_{sub.2}) \dots (N_{sub.r}) \bmod n, \text{ where:}$$

n is the same composite number as used for encryption;

wherein $r=2$.

2.-9. (Cancelled)

10. (Currently Amended) A system of claim 1, wherein at ~~least~~ least one encrypted version of the message is bypassed to a secret host that is not exposed to the public while the remaining are directed to ~~the~~ a main host, where the bypassed cipher versions are also collected from the secret host.

11. (Original) A system of claim 1, wherein redundant cipher versions of a message are generated and delivered to the destination, where they are identified and discarded before decryption.

Amendment - Serial No. 09/847,503.....Page 4

Docket No. SHAI-11

12. (Original) A system of claim 10, wherein the cipher version received at a secret host is further encrypted in a symmetric key encryption method before sending it to the main host, where it is decrypted by the same symmetric key.

13. (Currently Amended) A system for sending messages over a communications channel, comprising ~~any of the following two options:~~

~~(a)~~ an encoder to transform a message M into two or more cipher versions M.sub.1, M.sub.2, . . . , M.sub.r as follows:

$$M.sub.1=(M.sup.(e.sub.1+t)) \bmod n$$

$$M.sub.2=(M.sup.(e.sub.2+t)) \bmod n$$

. . .

$$M.sub.r (M.sup.(e.sub.r+t)) \bmod n, \text{ where:}$$

t is a random number generated on an encrypting machine;

e.sub.1, e.sub.2, . . . , e.sub.r are encrypting key components computed according to the relations:

$$(e.sub.1).(d.sub.1)+(e.sub.2).(d.sub.2)+ \dots \\ +(e.sub.r).(d.sub.r)=(k.sub.1).(p-1).(q-1)+1$$

and

$$(d.sub.1)+(d.sub.2)+ \dots +(d.sub.r)=(k.sub.2).(p-1).(q-1);$$

p and q are prime numbers, and $n=p.q$;

k.sub.1 and k.sub.2 are suitable integers;

(d.sub.1), (d.sub.2), . . . , (d.sub.r) are components of ~~the~~ an other key used by ~~the~~ a recipient for decrypting the cipher versions into the original message;

Amendment – Serial No. 09/847,503.....Page 5

Docket No. SHAI-11

a decoder coupled to receive the cipher versions $M_{sub.1}$, $M_{sub.2}$, ..., $M_{sub.r}$ from the communications channel and to transform them back to the original message M , where M is a function of $M_{sub.1}$, $M_{sub.2}$, ..., $M_{sub.r}$ and computed as follows:

$$N_{sub.1} = ((M_{sub.1})_{sup.}(d_{sub.1})) \bmod n$$

$$N_{sub.2} = ((M_{sub.2})_{sup.}(d_{sub.2})) \bmod n$$

...

$$N_{sub.r} = ((M_{sub.r})_{sup.}(d_{sub.r})) \bmod n$$

$$M = (N_{sub.1})(N_{sub.2}) \dots (N_{sub.2} \dots r) \bmod n.$$

~~(b). an encoder to transform a message M into two or more cipher versions $M_{sub.1}$, $M_{sub.2}$, ..., $M_{sub.r}$ as follows:~~

~~—— $M_{sub.1} = M_{sup.}(e_{sub.1}) \bmod n$~~

~~—— $M_{sub.2} = M_{sup.}(e_{sub.2}) \bmod n$~~

~~—— ...~~

~~—— $M_{sub.r} = M_{sup.}(e_{sub.r}) \bmod n$, where:~~

~~—— $e_{sub.1}$, $e_{sub.2}$, ..., $e_{sub.r}$ are encrypting key~~

~~components computed according to the following relation and conditions:~~

~~—— $(e_{sub.1})(d_{sub.1}) + (e_{sub.2})(d_{sub.2}) + \dots$~~

~~$+ (e_{sub.r})(d_{sub.r}) = (k_{sub.1})(p-1)(q-1) + 1$ and each of the~~

~~values $(e_{sub.1})$, $(e_{sub.2})$, ..., $(e_{sub.r})$ has a common factor~~

~~with $(p-1)(q-1)$, but there is no common factor for all the values~~

~~$(e_{sub.1})$, $(e_{sub.2})$, ..., $(e_{sub.r})$, and $(p-1)(q-1)$, where:~~

~~—— p and q are two prime numbers; $n = p \cdot q$;~~

Docket No. SHAI-11

~~— $k_{sub.1}$ is a suitable integer; and~~
~~— $(d_{sub.1}), (d_{sub.2}), \dots, (d_{sub.r})$ are decrypting key components used by the recipient for decrypting the cipher versions into the original message;~~
~~— a decoder coupled to receive the cipher versions $M_{sub.1}, M_{sub.2}, \dots, M_{sub.r}$ from the communications channel and to transform them back to the original message M , where M is a function of $M_{sub.1}, M_{sub.2}, \dots, M_{sub.r}$ and computed as follows:~~
~~— $N_{sub.1} = ((M_{sub.1})^{sup.(d_{sub.1})}) \bmod n$~~
~~— $N_{sub.2} = ((M_{sub.2})^{sup.(d_{sub.2})}) \bmod n$~~
~~— \dots~~
~~— $N_{sub.r} = ((M_{sub.r})^{sup.(d_{sub.r})}) \bmod n$~~
~~— $M = (N_{sub.1}) \cdot (N_{sub.2}) \cdot \dots \cdot (N_{sub.r}) \bmod n$~~
wherein $r=2$.

14. (Currently Amended) A computer-readable medium having computer-executable instructions causing ~~the~~ a computer to compute the following: key components $(e_{sub.1}), (e_{sub.2}), \dots, (e_{sub.r})$ and $(d_{sub.1}), (d_{sub.2}), \dots, (d_{sub.r})$ according to the relations as follows:
 $(e_{sub.1}) \cdot (d_{sub.1}) + (e_{sub.2}) \cdot (d_{sub.2}) + \dots + (e_{sub.r}) \cdot (d_{sub.r}) = (k_{sub.1}) \cdot (p-1) \cdot (q-1) + 1$ and $(d_{sub.1}) + (d_{sub.2}) + \dots + (d_{sub.r}) = (k_{sub.2}) \cdot (p-1) \cdot (q-1)$,
 where: p and q are prime numbers; and $k_{sub.1}$ and $k_{sub.2}$ are suitable integers; cipher versions of the original message M as follows:

Amendment – Serial No. 09/847,503.....Page 7

Docket No. SHAI-11

$M_{sub.1} = (M_{sup.}(e_{sub.1} + t)) \bmod n$ $M_{sub.2} = (M_{sup.}(e_{sub.2} + t)) \bmod n \dots$
 $M_{sub.r} = (M_{sup.}(e_{sub.r} + t)) \bmod n$, where: t is a random number generated on
an encrypting machine and discarded after encryption is complete. original
 message as follows: $N_{sub.1} = ((M_{sub.1})_{sup.}(d_{sub.1})) \bmod n$
 $N_{sub.2} = ((M_{sub.2})_{sup.}(d_{sub.2})) \bmod n \dots N_{sub.r} = ((M_{sub.r})_{sup.}(d_{sub.r})) \bmod n$
 $M = (N_{sub.1}) \cdot (N_{sub.2}) \dots (N_{sub.r}) \bmod n$

15. (Cancelled)

16. (New) A method of sending a message over a network, comprising the steps of:

applying two components of an encryption key to a message to generate two ciphers, using two blind exponents of the encryption key, wherein the two blind exponents of the encryption key are generated by adding a random number to each of the two components of the encryption key;

discarding the random number;

sending the two ciphers across the network to a receiver.